

AO 106 (Rev. 04/10) Application for a Search Warrant

LODGED

OCT 23 2018

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

BY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)Black Dell Latitude E5450 Laptop with Service Tag Serial  
Number CR3LY52 in custody of HSI Seattle

Case No. MJ18-486

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Black Dell Latitude E5450 Laptop with Service Tag Serial Number CR3LY52 as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4) (B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT CAO TRIET (DAN) HUYNH, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

OCT 23, 2018

Judge's signature

City and state: SEATTLE, WASHINGTON

MARY ALICE THEILER, U.S. MAGISTRATE JUDGE

Printed name and title

2018R01231

**ATTACHMENT A**  
**ITEMS TO BE SEARCHED**

The following item to be searched and subsequently forensically examined is currently in the custody of HSI Seattle and was detained by United States Probation on or about October 17, 2018, from MARK EVERTT DREBLOW and is currently located in the secure office of HSI Seattle at 1000 Second Avenue, Suite 2300, Seattle, Washington 98104:

Black Dell Latitude E5450 Laptop with Service Tag Serial Number CR3LY52

**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found on the SUBJECT DEVICE:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media;

2. Letters, emails, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

3. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

4. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

6. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

1           b. Any digital devices used to facilitate the transmission, creation,  
2 display, encoding or storage of data, including word processing equipment, modems,  
3 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

4           c. Any magnetic, electronic, or optical storage device capable of  
5 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or  
6 memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera  
7 memory cards, media cards, electronic notebooks, and personal digital assistants;

8           d. Any documentation, operating logs and reference manuals regarding  
9 the operation of the digital device or software;

10          e. Any applications, utility programs, compilers, interpreters, and other  
11 software used to facilitate direct or indirect communication with the computer hardware,  
12 storage devices, or data to be searched;

13          f. Any physical keys, encryption devices, dongles and similar physical  
14 items that are necessary to gain access to the computer equipment, storage devices or  
15 data; and

16          g. Any passwords, password files, test keys, encryption codes or other  
17 information necessary to access the computer equipment, storage devices or data;

18          8. Evidence of who used, owned or controlled any seized digital device(s) at  
19 the time the things described in this warrant were created, edited, or deleted, such as logs,  
20 registry entries, saved user names and passwords, documents, and browsing history;

21          9. Evidence of malware that would allow others to control any seized digital  
22 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well  
23 as evidence of the presence or absence of security software designed to detect malware;  
24 as well as evidence of the lack of such malware;

25          10. Evidence of the attachment to the digital device(s) of other storage devices  
26 or similar containers for electronic evidence;

27          11. Evidence of counter-forensic programs (and associated data) that are  
28 designed to eliminate data from a digital device;

12. Evidence of times the digital device(s) was used;

13. Any other electronically stored information (ESI) from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

13. Communications concerning or intended to facilitate sexual contact with minors.

**THE SEIZURE OF DIGITAL DEVICES AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.**

**AFFIDAVIT**

STATE OF WASHINGTON

ss

COUNTY OF KING

I, CAO TRIET (DAN) HUYNH, being first duly sworn on oath, depose and say:

**I. INTRODUCTION**

1. I am a Special Agent (SA) with the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge (SAC), Seattle, Washington. I have been an agent with HSI since April 2010. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

2. I am a graduate of the Federal Law Enforcement Training Center (FLETC), ICE Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of previous search warrants, which involved child exploitation and/or child pornography offenses, and the search and seizure of computers, related peripherals, and computer media equipment. I am a member of the Seattle Internet Crimes Against Children Task Force, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. Before joining HSI, I worked for

1 the City of Port Townsend, Washington, Police Department as a police officer and  
2 detective for approximately nine years.

3 3. I make this Affidavit in support of an application under Rule 41 of the  
4 Federal Rules of Criminal Procedure for a warrant to search the following items more  
5 fully described in Attachment A for the things specified in Attachment B:

6 a. Black Dell Latitude E5450 Laptop with Service Tag Serial Number  
7 CR3LY52

8 The item to be searched (at times referred to as the "SUBJECT DEVICE"), more  
9 fully described in Attachment A to this Affidavit, is currently located in the secure office  
10 of the HSI Seattle, 1000 Second Avenue, Suite 2300, Seattle, Washington 98104.

11 4. The facts set forth in this Affidavit are based on my own personal  
12 knowledge; knowledge obtained from other individuals during my participation in this  
13 investigation, including other law enforcement officers; review of documents and records  
14 related to this investigation; communications with others who have personal knowledge  
15 of the events and circumstances described herein; and information gained through my  
16 training and experience.

17 5. Because this Affidavit is submitted for the limited purpose of providing  
18 sufficient facts necessary to determine whether there is probable cause in support of the  
19 application for a search warrant, it does not set forth each and every fact that I or others  
20 have learned during the course of this investigation. I have set forth only the facts that I  
21 believe are relevant to the determination of probable cause to believe that evidence,  
22 fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution  
23 of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography)  
24 will be found on the SUBJECT DEVICE.

## 25 II. BACKGROUND

### 26 MARK EVERETT DREBLOW

27 6. On or about August 31, 2005, MARK EVERETT DREBLOW was  
28 sentenced in the Western District of Washington by the Honorable Benjamin H. Settle,



1 United States District Judge, to 120 months' imprisonment followed by five years of  
2 supervised release after being convicted of Possession of Child Pornography in violation  
3 of 18 U.S.C. § 2252(a)(4)(B) and (b)(2).

4 7. After DREBLOW's release from incarceration, he was ordered to abide by  
5 all standard conditions, as well as the following special conditions while under  
6 supervision: actively participate and make reasonable progress in a mental health/sexual  
7 offender treatment program, which may include physiological testing; have no direct or  
8 indirect contact with minor children; submit to polygraph examination; abide by all  
9 lifestyle restrictions or treatment requirements imposed by the therapist; not possess any  
10 electronic device that communicates through a modem or have internet access; not  
11 possess and/or use pornographic material of any type as described by the treatment  
12 provider; submit to financial disclosure; submit to computer monitoring and notify the  
13 probation office of any computer software owned or operated by the defendant; not incur  
14 new credit charges or open additional lines of credit without approval of the probation  
15 officer; and register as a sexual offender. His term of supervised release commenced on  
16 June 16, 2014, in the Western District of Washington.

17 BRIAN KEVIN RUBENAKER

18 8. On or about June 5, 2006, BRIAN KEVIN RUBENAKER was sentenced  
19 in the Western District of Washington by the Honorable James L. Robart, United States  
20 District Judge, to 151 months imprisonment followed by three years supervised release  
21 after being convicted of Possession of Child Pornography in violation of 18 U.S.C. §  
22 2252(a)(4)(B), (b)(2) and 2256.

23 9. After RUBENAKER's release from incarceration, he was ordered to abide  
24 by all standard conditions, as well as the following special conditions of supervision:  
25 Abstain from alcohol use; submit to search; not possess sexually explicit images;  
26 participate in polygraph examinations; participate in a sexual deviancy evaluation;  
27 participate in sexual deviancy treatment; follow lifestyle restrictions; not frequent places  
28 where minors are known to congregate; have no contact with minors; preapproval of



1 residence; disclose all computer software purchases; participate in computer monitoring;  
2 financial disclosure. RUBENAKER's term of supervised release commenced on April  
3 20, 2016, in the Western District of Washington.

4 10. RUBENAKER also has 1998 Washington State convictions for Child  
5 Molestation in the First Degree and Rape of a Child in the Third Degree.

6 11. According to United States Probation Officer Lisa Combs, DREBLOW and  
7 RUBENAKER met during sex offender treatment and became close friends.

### 8 III. SUMMARY OF INVESTIGATION

9 12. On or about October 17, 2018, United States Probation Officers Combs and  
10 Angela McGlynn conducted a routine unannounced home visit at DREBLOW's  
11 residence located at 13005 East Gibson Road, Apartment #T236, Everett, Washington  
12 98204. During the visit, Officer Combs saw what appeared to be electrical cords under a  
13 couch cushion, which was askew and partially propped up. Officer Combs asked  
14 DREBLOW if they were cords, and he moved quickly to the couch to try to hide them.  
15 She also asked if there was a computer there, and DREBLOW removed a black Dell  
16 Latitude E5450 Laptop (the SUBJECT DEVICE). DREBLOW stated the SUBJECT  
17 DEVICE belonged to his friend, RUBENAKER, and that they shared the SUBJECT  
18 DEVICE.

19 13. DREBLOW appeared extremely uneasy and concerned. He admitted to  
20 being nervous and scared. DREBLOW stated that he had the SUBJECT DEVICE for  
21 approximately ten days and that it was not password protected. Officers Combs and  
22 McGlynn advised that while they did not know what was on the SUBJECT DEVICE,  
23 there were several options to address its possession, including a referral back to sex  
24 offender treatment. DREBLOW stated that there were pictures of nude children on the  
25 SUBJECT DEVICE. Officers Combs and McGlynn inquired about his well-being and  
26 instructed him to report to their office the following morning, October 18, 2018. They  
27 also seized the SUBJECT DEVICE and secured it at their office in Everett, Washington.  
28

1       14. In light of these events, Officer Combs contacted RUBENAKER and  
2 directed him to report to her office on October 18, 2018,

3       15. DREBLOW reported as directed and was taken into custody for an alleged  
4 violation of his conditions of supervision: namely, possessing an Internet-capable device,  
5 a laptop computer, without authorization.

6       16. RUBENAKER also reported as directed and met with Officers Combs and  
7 McGlynn. He was aware of the SUBJECT DEVICE being seized through his contact  
8 with DREBLOW. RUBENAKER was questioned about his emotional well-being. He  
9 made statements of regret and remorse and said that he wished he had made a better  
10 decision ten days ago. RUBENAKER stated he purchased the SUBJECT DEVICE  
11 approximately eight to ten days ago. When asked who used the SUBJECT DEVICE  
12 RUBENAKER stated that he and DREBLOW shared it.

13       17. That same afternoon, RUBENAKER was arrested at his home in Everett  
14 for an alleged violations of his conditions of supervision—namely, failing to follow all  
15 lifestyle restrictions and treatment requirements imposed by the defendant's therapist and  
16 failing to notify the probation officer of all computer software owned and operated.

17       18. On or about October 19, 2018, I arrived at the United States Probation  
18 Office in Everett, Washington, and met with Officer Combs. I confirmed and obtained  
19 additional details of Officers Combs's and McGlynn's involvement in the case and took  
20 custody of the SUBJECT DEVICE.

21       19. The SUBJECT DEVICE was not manufactured in the state of Washington.  
22 On the back of the SUBJECT DEVICE, there is a Dell label that has "Made in China"  
23 printed on it.

#### 24                   IV. DEFINITIONS AND TECHNICAL TERMS

25       20. Set forth below are some definitions of technical terms, most of which are  
26 used throughout this Affidavit pertaining to the Internet and computers generally:

27           a. Computers and digital devices: As used in this Affidavit, the terms  
28 "computer" and "digital device," along with the terms "electronic storage media,"

1 “digital storage media,” and “data storage device,” refer to those items capable of storing,  
2 creating, transmitting, displaying, or encoding electronic or digital data, including  
3 computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart  
4 cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks  
5 and tablets, smart phones and personal digital assistants, printers, scanners, and other  
6 similar items.

7 b. Internet Service Providers (ISPs) and the storage of ISP records:

8 Internet Service Providers are commercial organizations that are in business to provide  
9 individuals and businesses access to the Internet. ISPs provide a range of functions for  
10 their customers including access to the Internet, web hosting, e mail, remote storage, and  
11 co-location of computers and other communications equipment. ISPs maintain records  
12 (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers  
13 are individuals or entities). These records may include account application information,  
14 subscriber and billing information, account access information (often times in the form of  
15 log files), e mail communications, information concerning content uploaded and/or stored  
16 on or via the ISP's servers, and other information, which may be stored both in computer  
17 data format and in written or printed record format. ISPs reserve and/or maintain  
18 computer disk storage space on their computer system for their subscribers' use.

19 c. Internet Protocol (IP) Address: Typically, computers or devices on  
20 the Internet are referenced by a unique Internet Protocol address the same way every  
21 telephone has a unique telephone number. An IP address consists of four numeric  
22 sequences, separated by a period, and each numeric sequence is a whole number between  
23 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual  
24 accesses the Internet, the computer from which that individual initiates access is assigned  
25 an IP address. A central authority provides each ISP a limited block of IP addresses for  
26 use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing,  
27 that is, they allocate any unused IP address at the time of initiation of an Internet session  
28 each time a customer or subscriber accesses the Internet. A dynamic IP address is

1 reserved by an ISP to be shared among a group of computers over a period of time. The  
2 ISP logs the date, time, and duration of the Internet session for each IP address and can  
3 identify the user of that IP address for such a session from these records. Typically, users  
4 who sporadically access the Internet via a dial up modem will be assigned an IP address  
5 from a pool of IP addresses for the duration of each dial up session. Once the session  
6 ends, the IP address is available for the next dial up customer. On the other hand, some  
7 ISPs, including some cable providers, employ static IP addressing, that is, a customer or  
8 subscriber's computer is assigned one IP address that is used to identify each and every  
9 Internet session initiated through that computer. In other words, a static IP address is an  
10 IP address that does not change over a period of time and is typically assigned to a  
11 specific computer.

12 d. Hash Value: "Hashing" refers to the process of using a  
13 mathematical function, often called an algorithm, to generate a numerical identifier for  
14 data. This numerical identifier is called a "hash value" and can be thought of as a "digital  
15 fingerprint" for data. If the data that has been "hashed" is changed, even very slightly  
16 (like through the addition or deletion of a comma or a period in a text file), the hash value  
17 for that data would change. Therefore, if a file such as a digital photo is a hash value  
18 match to a known file, it means that the digital photo is an exact copy of the known file.

## 19 V. TECHNICAL BACKGROUND

20 21. As part of my training, I have become familiar with the Internet, a global  
21 network of computers and other electronic devices that communicate with each other  
22 using various means, including standard telephone lines, high speed telecommunications  
23 links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite.  
24 Due to the structure of the Internet, connections between computers on the Internet  
25 routinely cross state and international borders, even when the computers communicating  
26 with each other are in the same state. Individuals and entities use the Internet to gain  
27 access to a wide variety of information; to send information to, and receive information  
28

1 from, other individuals; to conduct commercial transactions; and to communicate via  
2 email.

3 22. I know, based on my training and experience, that cellular phones (referred  
4 to generally as "smart phones") have the capability to access the Internet and store  
5 information, such as videos and images. As a result, an individual using a smart phone  
6 can send, receive, and store files, including child pornography, without accessing a  
7 personal computer or laptop. An individual using a smart phone can also easily plug the  
8 device into a computer, via a USB cable, and transfer data files from one digital device to  
9 another. Many people generally carry their smart phone on their person; recent  
10 investigations in this District have resulted in the discovery of child pornography files on  
11 smart phones which were carried on an individual's person at the time the phones were  
12 seized.

13 23. As set forth above and in Attachment B to this Affidavit, I seek permission  
14 to search for and seize evidence, fruits, and instrumentalities of the above-referenced  
15 crimes that might be on the SUBJECT DEVICE, in whatever form they are found. It has  
16 been my experience that individuals involved in child pornography often prefer to store  
17 images of child pornography in electronic form. The ability to store images of child  
18 pornography in electronic form makes digital devices, examples of which are enumerated  
19 in Attachment B to this Affidavit, an ideal repository for child pornography because the  
20 images can be easily sent or received over the Internet. As a result, one form in which  
21 these items may be found is as electronic evidence stored on a digital device.

22 a. Based upon my knowledge, training, and experience in child  
23 exploitation and child pornography investigations, and the experience and training of  
24 other law enforcement officers with whom I have had discussions, I know that computers  
25 and computer technology have revolutionized the way in which child pornography is  
26 collected, distributed, and produced. Prior to the advent of computers and the Internet,  
27 child pornography was produced using cameras and film, resulting in either still  
28 photographs or movies. The photographs required darkroom facilities and a significant

1 amount of skill in order to develop and reproduce the images. As a result, there were  
2 definable costs involved with the production of pornographic images. To distribute these  
3 images on any scale also required significant resources. The photographs themselves  
4 were somewhat bulky and required secure storage to prevent their exposure to the public.  
5 The distribution of these images was accomplished through a combination of personal  
6 contacts, mailings, and telephone calls, and compensation would follow the same paths.  
7 More recently, through the use of computers and the Internet, distributors of child  
8 pornography use membership based/subscription based websites to conduct business,  
9 allowing them to remain relatively anonymous.

10           b. In addition, based upon my own knowledge, training, and experience  
11 in child exploitation and child pornography investigations, and the experience and  
12 training of other law enforcement officers with whom I have had discussions, I know that  
13 the development of computers has also revolutionized the way in which those who seek  
14 out child pornography are able to obtain this material. Computers serve four basic  
15 functions in connection with child pornography: production, communication, distribution,  
16 and storage. More specifically, the development of computers has changed the methods  
17 used by those who seek to obtain access to child pornography as described in  
18 subparagraphs (c) through (f) below.

19           c. Producers of child pornography can now produce both still and  
20 moving images directly from the average video or digital camera. These still and/or  
21 moving images are then uploaded from the camera to the computer, either by attaching  
22 the camera to the computer through a USB cable or similar device, or by ejecting the  
23 camera memory card from the camera and inserting it into a card reader. Once uploaded  
24 to the computer, the images can then be stored, manipulated, transferred, or printed  
25 directly from the computer. Images can be edited in ways similar to those by which a  
26 photograph may be altered. Images can be lightened, darkened, cropped, or otherwise  
27 manipulated. Producers of child pornography can also use a scanner to transfer printed  
28 photographs into a computer-readable format. As a result of this technology, it is



1 relatively inexpensive and technically easy to produce, store, and distribute child  
2 pornography. In addition, there is an added benefit to the pornographer in that this  
3 method of production does not leave as large a trail for law enforcement to follow.

4 d. The Internet allows any computer to connect to another computer.  
5 By connecting to a host computer, electronic contact can be made to literally millions of  
6 computers around the world. A host computer is one that is attached to a network and  
7 serves many users. Host computers, including ISPs, allow email service between  
8 subscribers and sometimes between their own subscribers and those of other networks.  
9 In addition, these service providers act as a gateway for their subscribers to the Internet.  
10 Having said that, however, this application does not seek to reach any host computers.  
11 This application seeks permission only to search the SUBJECT DEVICE.

12 e. The Internet allows users, while still maintaining anonymity, to  
13 easily locate (i) other individuals with similar interests in child pornography, and (ii)  
14 websites that offer images of child pornography. Those who seek to obtain images or  
15 videos of child pornography can use standard Internet connections, such as those  
16 provided by businesses, universities, and government agencies, to communicate with  
17 each other and to distribute child pornography. These communication links allow  
18 contacts around the world as easily as calling next door. Additionally, these  
19 communications can be quick, relatively secure, and as anonymous as desired. All of  
20 these advantages, which promote anonymity for both the distributor and recipient, are  
21 well known and are the foundation of transactions involving those who wish to gain  
22 access to child pornography over the Internet. Sometimes the only way to identify both  
23 parties and verify the transportation of child pornography over the Internet is to examine  
24 the distributor's/recipient's computer, including the Internet history and cache to look for  
25 "footprints" of the websites and images accessed by the distributor/recipient.

26 f. The computer's capability to store images in digital form makes it an  
27 ideal repository for child pornography. The size of the electronic storage media  
28 (commonly referred to as a "hard drive") used in home computers has grown



1 tremendously within the last several years. Hard drives with the capacity of 2 terabytes  
2 are not uncommon. These drives can store thousands of images at very high resolution.  
3 Magnetic storage located in host computers adds another dimension to the equation. It is  
4 possible to use a video camera to capture an image, process that image in a computer  
5 with a video capture board, and save that image to storage elsewhere. Once this is done,  
6 there is no readily apparent evidence at the "scene of the crime." Only with careful  
7 laboratory examination of electronic storage devices is it possible to recreate the evidence  
8 trail.

9       24. Based upon my knowledge, experience, and training in child pornography  
10 investigations, and the training and experience of other law enforcement officers with  
11 whom I have had discussions, I know that there are certain characteristics common to  
12 individuals who have a sexualized interest in children and depictions of children:

13           a. They may receive sexual gratification, stimulation, and satisfaction  
14 from contact with children; or from fantasies they may have viewing children engaged in  
15 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other  
16 visual media; or from literature describing such activity.

17           b. They may collect sexually explicit or suggestive materials in a  
18 variety of media, including photographs, magazines, motion pictures, videotapes, books,  
19 slides, and/or drawings or other visual media. Such individuals often times use these  
20 materials for their own sexual arousal and gratification. Further, they may use these  
21 materials to lower the inhibitions of children they are attempting to seduce, to arouse the  
22 selected child partner, or to demonstrate the desired sexual acts. These individuals may  
23 keep records, to include names, contact information, and/or dates of these interactions, of  
24 the children they have attempted to seduce, arouse, or with whom they have engaged in  
25 the desired sexual acts.

26           c. They often maintain any "hard copies" of child pornographic  
27 material that is, their pictures, films, video tapes, magazines, negatives, photographs,  
28 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

1 their home or some other secure location. These individuals typically retain these "hard  
2 copies" of child pornographic material for many years, as they are highly valued.

3 d. Likewise, they often maintain their child pornography collections  
4 that are in a digital or electronic format in a safe, secure and private environment, such as  
5 a computer and surrounding area. These collections are often maintained for several  
6 years and are kept close by, often at the individual's residence or some otherwise easily  
7 accessible location, to enable the owner to view the collection, which is valued highly.  
8 They also may opt to store the contraband in cloud accounts. Cloud storage is a model of  
9 data storage where the digital data is stored in logical pools, the physical storage can span  
10 multiple servers, and often locations, and the physical environment is typically owned  
11 and managed by a hosting company. Cloud storage allows the offender ready access to  
12 the material from any device that has an Internet connection, worldwide, while also  
13 attempting to obfuscate or limit the criminality of possession as the material is stored  
14 remotely and not on the offender's device.

15 e. They also may correspond with and/or meet others to share  
16 information and materials; rarely destroy correspondence from other child pornography  
17 distributors/collectors; conceal such correspondence as they do their sexually explicit  
18 material; and often maintain lists of names, addresses, and telephone numbers of  
19 individuals with whom they have been in contact and who share the same interests in  
20 child pornography.

21 f. They generally prefer not to be without their child pornography for  
22 any prolonged time period. This behavior has been documented by law enforcement  
23 officers involved in the investigation of child pornography throughout the world.

24 25. In addition to offenders who collect and store child pornography, law  
25 enforcement has encountered offenders who obtain child pornography from the internet,  
26 view the contents and subsequently delete the contraband, often after engaging in self-  
27 gratification. In light of technological advancements, increasing Internet speeds and  
28 worldwide availability of child sexual exploitative material, this phenomenon offers the

1 offender a sense of decreasing risk of being identified and/or apprehended with quantities  
2 of contraband. This type of consumer is commonly referred to as a 'seek and delete'  
3 offender, knowing that the same or different contraband satisfying their interests remain  
4 easily discoverable and accessible online for future viewing and self-gratification. I  
5 know that, regardless of whether a person discards or collects child pornography he/she  
6 accesses for purposes of viewing and sexual gratification, evidence of such activity is  
7 likely to be found on computers and related digital devices, including storage media, used  
8 by the person. This evidence may include the files themselves, logs of account access  
9 events, contact lists of others engaged in trafficking of child pornography, backup files,  
10 and other electronic artifacts that may be forensically recoverable.

11       26. Given the above-stated facts, including DREBLOW and RUBENAKER's  
12 criminal histories and the findings of United States Probation, and based on my  
13 knowledge, training and experience, along with my discussions with other law  
14 enforcement officers who investigate child exploitation crimes, I believe that DREBLOW  
15 and RUBENAKER likely have a sexualized interest in children and depictions of  
16 children and that evidence of child pornography is likely to be found on the SUBJECT  
17 DEVICE.

18       27. Based on my training and experience, and that of computer forensic agents  
19 that I work and collaborate with on a daily basis, I know that every type and kind of  
20 information, data, record, sound or image can exist and be present as electronically stored  
21 information on any of a variety of computers, computer systems, digital devices, and  
22 other electronic storage media. I also know that electronic evidence can be moved easily  
23 from one digital device to another. As a result, I believe that electronic evidence may be  
24 stored on the SUBJECT DEVICE.

25       28. Based on my training and experience, and my consultation with computer  
26 forensic agents who are familiar with searches of computers, I know that in some cases  
27 the items set forth in Attachment B may take the form of files, documents, and other data  
28 that is user-generated and found on a digital device. In other cases, these items may take

1 the form of other types of data – including in some cases data generated automatically by  
2 the devices themselves.

3 29. Based on my training and experience, and my consultation with computer  
4 forensic agents who are familiar with searches of computers, I believe that regarding any  
5 digital devices recovered from DREBLOW and RUBENAKER there is probable cause to  
6 believe that the items set forth in Attachment B will be stored in the SUBJECT DEVICE  
7 for a number of reasons, including but not limited to the following:

8 a. Once created, electronically stored information (ESI) can be stored  
9 for years in very little space and at little or no cost. A great deal of ESI is created, and  
10 stored, moreover, even without a conscious act on the part of the device operator. For  
11 example, files that have been viewed via the Internet are sometimes automatically  
12 downloaded into a temporary Internet directory or “cache,” without the knowledge of the  
13 device user. The browser often maintains a fixed amount of hard drive space devoted to  
14 these files, and the files are only overwritten as they are replaced with more recently  
15 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may  
16 include relevant and significant evidence regarding criminal activities, but also, and just  
17 as importantly, may include evidence of the identity of the device user, and when and  
18 how the device was used. Most often, some affirmative action is necessary to delete ESI.  
19 And even when such action has been deliberately taken, ESI can often be recovered,  
20 months or even years later, using forensic tools.

21 b. Wholly apart from data created directly (or indirectly) by user-  
22 generated files, digital devices – in particular, a computer’s internal hard drive – contain  
23 electronic evidence of how a digital device has been used, what it has been used for, and  
24 who has used it. This evidence can take the form of operating system configurations,  
25 artifacts from operating systems or application operations, file system data structures, and  
26 virtual memory “swap” or paging files. Computer users typically do not erase or delete  
27 this evidence, because special software is typically required for that task. However, it is  
28 technically possible for a user to use such specialized software to delete this type of

1 information – and, the use of such special software may itself result in ESI that is relevant  
2 to the criminal investigation. HSI agents in this case have consulted on computer  
3 forensic matters with law enforcement officers with specialized knowledge and training  
4 in computers, networks, and Internet communications. In particular, to properly retrieve  
5 and analyze electronically stored (computer) data, and to ensure accuracy and  
6 completeness of such data and to prevent loss of the data either from accidental or  
7 programmed destruction, it is necessary to conduct a forensic examination of the  
8 computers. To effect such accuracy and completeness, it may also be necessary to  
9 analyze not only data storage devices, but also peripheral devices which may be  
10 interdependent, the software to operate them, and related instruction manuals containing  
11 directions concerning operation of the computer and software.

## 12 VI. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

13 30. In addition, based on my training and experience and that of computer  
14 forensic agents that I work and collaborate with on a daily basis, I know that in most  
15 cases it is impossible to successfully conduct a complete, accurate, and reliable search for  
16 electronic evidence stored on a digital device during the physical search of a search site  
17 for a number of reasons, including but not limited to the following:

18 a. Technical Requirements: Searching digital devices for criminal  
19 evidence is a highly technical process requiring specific expertise and a properly  
20 controlled environment. The vast array of digital hardware and software available  
21 requires even digital experts to specialize in particular systems and applications, so it is  
22 difficult to know before a search which expert is qualified to analyze the particular  
23 system(s) and electronic evidence found at a search site. As a result, it is not always  
24 possible to bring to the search site all of the necessary personnel, technical manuals, and  
25 specialized equipment to conduct a thorough search of every possible digital  
26 device/system present. In addition, electronic evidence search protocols are exacting  
27 scientific procedures designed to protect the integrity of the evidence and to recover even  
28 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is



1 extremely vulnerable to inadvertent or intentional modification or destruction (both from  
2 external sources or from destructive code embedded in the system such as a “booby  
3 trap”), a controlled environment is often essential to ensure its complete and accurate  
4 analysis.

5           b.     Volume of Evidence: The volume of data stored on many digital  
6 devices is typically so large that it is impossible to search for criminal evidence in a  
7 reasonable period of time during the execution of the physical search of a search site. A  
8 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A  
9 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000  
10 double-spaced pages of text. Computer hard drives are now being sold for personal  
11 computers capable of storing up to two terabytes (2,000 gigabytes of data.) Additionally,  
12 this data may be stored in a variety of formats or may be encrypted (several new  
13 commercially available operating systems provide for automatic encryption of data upon  
14 shutdown of the computer).

15           c.     Search Techniques: Searching the ESI for the items described in  
16 Attachment B may require a range of data analysis techniques. In some cases, it is  
17 possible for agents and analysts to conduct carefully targeted searches that can locate  
18 evidence without requiring a time-consuming manual search through unrelated materials  
19 that may be commingled with criminal evidence. In other cases, however, such  
20 techniques may not yield the evidence described in the warrant, and law enforcement  
21 personnel with appropriate expertise may need to conduct more extensive searches, such  
22 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to  
23 determine whether it falls within the scope of the warrant.

24           31.     In this particular case, the government anticipates the use of a hash value  
25 library to exclude normal operating system files that do not need to be searched, which  
26 will facilitate the search for evidence that does come within the items described in  
27 Attachment B. Further, the government anticipates the use of hash values and known file  
28 filters to assist the digital forensics examiners/agents in identifying known and or

1 suspected child pornography image files. Use of these tools will allow for the quick  
2 identification of evidentiary files but also assist in the filtering of normal system files that  
3 would have no bearing on the case.

4 32. In accordance with the information in this Affidavit, law enforcement  
5 personnel will execute the search of digital devices seized pursuant to this warrant as  
6 follows:

7 a. In order to examine the ESI in a forensically sound manner, law  
8 enforcement personnel with appropriate expertise will produce a complete forensic  
9 image, if possible and appropriate, of any digital device that is found to contain data or  
10 items that fall within the scope of Attachment B of this Affidavit. In addition,  
11 appropriately trained personnel may search for and attempt to recover deleted, hidden, or  
12 encrypted data to determine whether the data fall within the list of items to be seized  
13 pursuant to the warrant. In order to search fully for the items identified in the warrant,  
14 law enforcement personnel, which may include investigative agents, may then examine  
15 all of the data contained in the forensic image/s and/or on the digital devices to view their  
16 precise contents and determine whether the data fall within the list of items to be seized  
17 pursuant to the warrant.

18 b. The search techniques that will be used will be only those methodologies,  
19 techniques and protocols as may reasonably be expected to find, identify, segregate  
20 and/or duplicate the items authorized to be seized pursuant to Attachment B to this  
21 Affidavit.

22 c. If, after conducting its examination, law enforcement personnel determine  
23 that any digital device is an instrumentality of the criminal offenses referenced above, the  
24 government may retain that device during the pendency of the case as necessary to,  
25 among other things, preserve the instrumentality evidence for trial, ensure the chain of  
26 custody, and litigate the issue of forfeiture.

27 33. In order to search for ESI that falls within the list of items to be seized  
28 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and



1 search the following items (heretofore and hereinafter referred to as "digital devices"),  
2 subject to the procedures set forth above:

3 a. Any digital device capable of being used to commit, further, or store  
4 evidence of the offense(s) listed above;

5 b. Any digital device used to facilitate the transmission, creation,  
6 display, encoding, or storage of data, including word processing equipment, modems,  
7 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

8 c. Any magnetic, electronic, or optical storage device capable of  
9 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or  
10 memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera  
11 memory cards, media cards, electronic notebooks, and personal digital assistants;

12 d. Any documentation, operating logs and reference manuals regarding  
13 the operation of the digital device, or software;

14 e. Any applications, utility programs, compilers, interpreters, and other  
15 software used to facilitate direct or indirect communication with the device hardware, or  
16 ESI to be searched;

17 f. Any physical keys, encryption devices, dongles and similar physical  
18 items that are necessary to gain access to the digital device, or ESI; and

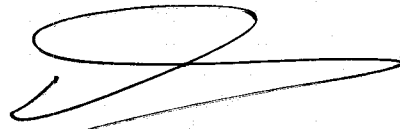
19 g. Any passwords, password files, test keys, encryption codes or other  
20 information necessary to access the digital device or ESI.

## 21 VII. INSTRUMENTALITIES

22 34. Based on the information in this Affidavit, I also believe that the SUBJECT  
23 DEVICE are instrumentalities of crime and constitute the means by which violations of  
24 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. §  
25 2252(a)(4)(B) (Possession of Child Pornography) have been committed. Therefore, I  
26 believe that in addition to seizing the digital devices to conduct a search of their contents  
27 as set forth herein, there is probable cause to seize those digital devices as  
28 instrumentalities of criminal activity.

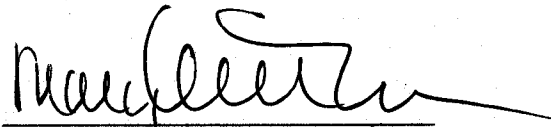
**VIII. CONCLUSION**

35. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located on the SUBJECT DEVICE, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the SUBJECT DEVICE, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.



CAO TRIET (DAN) HUYNH,  
Affiant, Special Agent  
Department of Homeland Security  
Homeland Security Investigations

SUBSCRIBED and SWORN to before me this 23 day of October, 2018.



MARY ALICE THEILER  
United States Magistrate Judge

**ATTACHMENT A**  
**ITEMS TO BE SEARCHED**

The following item to be searched and subsequently forensically examined is currently in the custody of HSI Seattle and was detained by United States Probation on or about October 17, 2018, from MARK EVERTT DREBLOW and is currently located in the secure office of HSI Seattle at 1000 Second Avenue, Suite 2300, Seattle, Washington 98104:

Black Dell Latitude E5450 Laptop with Service Tag Serial Number CR3LY52

**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found on the SUBJECT DEVICE:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media;

2. Letters, emails, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

3. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

4. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

6. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

1           b. Any digital devices used to facilitate the transmission, creation,  
2 display, encoding or storage of data, including word processing equipment, modems,  
3 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

4           c. Any magnetic, electronic, or optical storage device capable of  
5 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or  
6 memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera  
7 memory cards, media cards, electronic notebooks, and personal digital assistants;

8           d. Any documentation, operating logs and reference manuals regarding  
9 the operation of the digital device or software;

10          e. Any applications, utility programs, compilers, interpreters, and other  
11 software used to facilitate direct or indirect communication with the computer hardware,  
12 storage devices, or data to be searched;

13          f. Any physical keys, encryption devices, dongles and similar physical  
14 items that are necessary to gain access to the computer equipment, storage devices or  
15 data; and

16          g. Any passwords, password files, test keys, encryption codes or other  
17 information necessary to access the computer equipment, storage devices or data;

18          8. Evidence of who used, owned or controlled any seized digital device(s) at  
19 the time the things described in this warrant were created, edited, or deleted, such as logs,  
20 registry entries, saved user names and passwords, documents, and browsing history;

21          9. Evidence of malware that would allow others to control any seized digital  
22 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well  
23 as evidence of the presence or absence of security software designed to detect malware;  
24 as well as evidence of the lack of such malware;

25          10. Evidence of the attachment to the digital device(s) of other storage devices  
26 or similar containers for electronic evidence;

27          11. Evidence of counter-forensic programs (and associated data) that are  
28 designed to eliminate data from a digital device;

1           12. Evidence of times the digital device(s) was used;

2           13. Any other electronically stored information (ESI) from the digital device(s)  
3 necessary to understand how the digital device was used, the purpose of its use, who used  
4 it, and when.

5           13. Communications concerning or intended to facilitate sexual contact with  
6 minors.

7  
8  
9 **THE SEIZURE OF DIGITAL DEVICES AND/OR THEIR COMPONENTS AS**  
10 **SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH**  
11 **WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES**  
12 **CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY**  
13 **DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING**  
14 **OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE,**  
15 **INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.**  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28